IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF APPLE IPHONE CELLULAR TELEPHONE CURRENTLY LOCATED AT 1000 ELM STREET, MANCHESTER, NH 03101	Case No. 19-mj-119-01-AJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, George Jasek III, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Secret Service, and have been so employed since March 5, 2018. I am currently assigned to the Manchester, New Hampshire Resident Office. In preparation for my employment with the Secret Service, I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia. I also completed the Special Agent Training Course at the Secret Service's James J. Rowley Training Center in Laurel, Maryland. In addition to these training programs, I have completed numerous in-service training courses related to constitutional law. Prior to becoming a Special Agent, I was a Police Officer in Nashua, New Hampshire for approximately

5 years. My present duties include the investigation of federal offenses, including, but not limited to, those involving financial fraud and its related activities.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a white Apple iPhone with no external model number or serial numbers but marked for identification, hereinafter the "Device." The Device is currently located in the Secret Service evidence room located at 1000 Elm Street, Manchester, NH 03101.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On Friday, April 26, 2019, the Hudson Police Department received a phone call from a S.W., who observed a black Chevrolet Malibu with New Jersey license plates approach the ATM located at a Digital Federal Credit Union ("DCU") in Hudson, New Hampshire. She explained that she saw the operator of the vehicle use the ATM three separate occasions, each time leaving the ATM when another vehicle pulled in behind him, circling the bank, and getting back in line.

7. Accounts at DCU are federally insured by the National Credit Union Share Insurance Fund.

8. Hudson Police Officer Robert McNally responded to the report of suspicious activity and arrived at the Hudson DCU almost an hour after the report of suspicious activity. He found the black Chevrolet Malibu at the DCU ATM. Officer McNally approached the vehicle and observed through the passenger side window a large sum of U.S. currency on the front passenger seat, several cards on the center console, and several sets of numbers on the screen of a cellphone that the operator of the vehicle was holding. The operator of the vehicle, Syed Hoque (DOB: [redacted]995) initially stated that the money was for his girlfriend and the cards did not belong to him. When asked who owned the cards, Hoque said "I don't know I'm supposed to give them to another guy," adding that he acquired them from someone in New York and was supposed to deliver them to someone else. When asked about the reason for having such a large sum of money, he at first stated that he emptied his life savings for while he was in New Hampshire, then later said that it was money sent to him from people he knows all over the world.

9. The Hudson police seized Hoque's cell phone and vehicle to preserve evidence while they applied for search warrants. They allowed Hoque to call a friend to arrange for a ride. After the call, Hoque said that a friend, "T" would pick him up and that the best number to reach him was T's number: [redacted]4607. Officer McNally gave Hoque his business card and left.

10. Later, at about 2:30am on April 27, 2019, Officer McNally received a call from Hoque who said that he wanted to talk further. Officer McNally transported Hoque to Hudson Police Department, where Hoque explained that he is associated with an unknown source named "D", who is located outside of the United States. The operation that "D" leads uses manipulated gift cards to acquire money from ATMs. Hoque is working with two men in New Hampshire,

"A.J." and "T", who he met through "D", and rented room #510 with them at the Days Hotel and Conference Center in Methuen, Massachusetts.

11. Hoque further explained that their operation involves a reconnaissance to identify ATMs that will accept manipulated gift cards, while "A.J." and "T" use an "MSR machine" to perform the manipulation. Based on my training and experience, "MSR" stands for "Magnetic Stripe Reader" and an MSR machine can read and write the information stored in the magnetic stripe on the back of credit and debit cards. With such a machine, individuals can encode stolen credit and debit card information onto blank credit and debit or gift cards.

12. Hoque said they would begin by going to all of the Digital Federal Credit Union branches within a 25 mile radius of their hotel, conduct withdrawals starting at 10:15pm, acquire as much money as possible, then return to the hotel to count how much was taken. Lastly, on the night he was stopped by Hudson Police, Hoque was to meet with "A.J.", "T" and a third associate to receive the sum of the money collected over the previous three days. After receiving the money, Hoque was to drive back to New York and launder it through a local casino, eventually giving the money to another associate who would facilitate its delivery across the border to "D".

13. On Saturday, April 27, 2018, at approximately 5:00am, Officer McNally and Detective Dang of the Hudson Police Department contacted Detective Sean Fountain of the Methuen Massachusetts Police Department regarding the thefts from ATMs. Officer McNally reported that he had responded to a suspicious activity call at the DCU located at 254 Lowell Road in Hudson, New Hampshire.

14. Officer McNally reported to Detective Fountain that Hoque stated he works with a group of individuals who are connected to thefts from ATMs. Detective Fountain was also

advised by Officer McNally that Hoque stated he works with three other men in the New Hampshire area who manipulate cards into looking like an ATM card/debit card in order to withdraw money from DCU branches at approximately 10:15 every night. Officer McNally explained that Hoque reported the ring operates out of the Days Inn Hotel in Methuen, Massachusetts where the money is counted and transported to New York. Detective Fountain was also advised by Officer McNally that Hoque also stated the money is then "cleaned" at a casino in New York before being transported to Canada, where the operation is managed.

15. According to Methuen Police Department report number 1900012236-00036816, Hoque stated that one of the individuals he is working with, Tharushan Nirmalachandran, was renting a room at the Days Inn Hotel at 159 Pelham Street in Methuen, Massachusetts. Hotel staff at the Days Inn Hotel confirmed that, at the time Hoque provided this information, Nirmalachandran was renting room 510 at the hotel.

16. Detective Fountain applied for and was granted a search warrant by The Commonwealth of Massachusetts Lawrence District Court for room 510 at the Days Inn hotel. Upon entering the room, two individuals, later identified as Nirmalachandran and Ajitharan Raveendran, were in the room. Nirmalachandran and Raveendran stated that they were in the United States of America visiting from Canada.

17. The Methuen Police Department contacted Homeland Security/ICE to assist with identifying the two individuals. Homeland Security/ICE identified the two subjects as Tharushan Nirmalachandran (DOB: [redacted] 1989) of Quebec, Canada and Ajitharan Raveendran (DOB: [redacted] 1990) of Montreal, Canada.

18. During the execution of the search warrant of room 510 at the Days Inn Hotel, the Methuen Police Department located two cellular phones, one Canadian identification card, and

keys to a rental car that were in the possession of Nirmalachandran. The rental vehicle was located in the parking lot area of the Days Inn hotel and towed to the Methuen Police Department.

19. Detective Fountain applied for and was granted a search warrant by The Commonwealth of Massachusetts Lawrence District Court for the vehicle rented by Nirmalachandran. The vehicle was identified as a 2018 Nissan Versa bearing New York registration number [redacted]670 with a Vehicle Identification Number (VIN) of [redacted]040. The vehicle is owned by Hertz Vehicles LLC. The following is a list of items located in the trunk of the vehicle:

- One (1) portable credit card programmer MSR (Magnetic Stripe Reader) X6
- Ninety five (95) Visa gift card packaging
- One hundred and three (103) Gift cards (Visa, American Express, MasterCard)
- $51,610 United States Currency
- Three (3) receipts
- Three (3) Delta Airlines travel tickets
- One (1) Hewlett Packard (HP) laptop computer
- One (1) Holiday Inn receipt

20. Detective Fountain's investigation revealed that Raveendran had also rented a vehicle and it was located in the parking lot area of the Days Inn Hotel. Detective Fountain applied for and was granted a search warrant by The Commonwealth of Massachusetts Lawrence District Court for this rental vehicle in Raveendran's name. The vehicle was a grey 2017

Hyundai Elantra which is owned by Hertz Vehicles LLC. Located within the Hyundai Elantra was a wallet believed to be Raveendran's which contained $451 in United States currency.

21. Officer Elvin Alarcon of the Methuen Police Department subsequently reviewed Days Inn Hotel surveillance footage recorded the morning of April 27, 2019, prior to the execution of the Massachusetts search warrants. Officer Alarcon identified both Nirmalachandran and Raveendran carrying large duffel bags from room number 510. Detective Fountain informed me that the bags Nirmalachandran and Raveendran were carrying on video surveillance were similar to the type of bags found in the trunk of the Nissan Versa rental vehicle. I later reviewed the same footage and confirmed that the bags were brought from the rear of the hotel to the parking lot.

22. The Device is currently in the lawful possession of the Secret Service. It came into the Secret Service's possession in the following way: On Thursday, May 2, 2019, I responded to the Hudson Police Department regarding the arrest of Hoque. Hudson Police Department had previously seized the Device during the arrest of Hoque and placed it in their inventory. Hudson Police Department subsequently transferred possession of the Device to the Secret Service. Therefore, while the Secret Service might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

23. The Device is currently in storage at 1000 Elm Street, Manchester, NH 03101. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Secret Service.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal

computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

25. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

NATURE AND MANNER OF SEARCH

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve

the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

31. As described in Attachment A, the Device is an Apple brand device, specifically an iPhone, but with no external model number.

32. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that some Apple devices offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. The biometric features available on the Device could include a fingerprint scanner, a facial recognition feature, and/or an iris recognition feature.

33. If the fingerprint scanner is enabled, a user can register multiple fingerprints that can be used to unlock the Device. To activate the fingerprint scanner, a user must use a registered fingerprint to unlock the Device by either pressing or swiping the relevant finger(s) to the device's fingerprint scanner. The Device will unlock if it detects a registered fingerprint.

34. If the facial recognition feature is enabled, a user can register his or her face to be used to unlock the Device. To activate the facial recognition feature, a user must hold the Device in front of his or her face. The Device's front-facing camera next analyzes and records data based on the user's facial characteristics. The Device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

35. If an iris recognition feature is enabled, a user can register one or both of his or her irises to be used to unlock the Device. To activate the iris recognition feature, the user holds the device in front of his or her face. The Device next directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's

irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises.

36. In my training and experience, users of electronic devices often enable the fingerprint scanner, facial recognition feature, and/or iris recognition feature because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

37. The passcode or password that would unlock the Device is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device, making the use of the device's biometric features necessary to the execution of the search authorized by this warrant.

38. I also know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that in some circumstances the Device cannot be unlocked via biometric features even if such features have been enabled. This can occur when the device has been restarted, inactive, or has not been unlocked for a certain period of time. Thus, the opportunity to unlock the Device through the fingerprint scanner, facial recognition feature, and/or iris recognition feature may exist for only a short time.

39. The Device was found in the possession of Hoque at the time of his initial stop by Hudson Police Department and later used to make a phone call. Additionally, the phone was seized and inventoried as belonging to Hoque following his arrest by Hudson Police Department. Based on these facts and my training and experience, it is likely that Hoque is the user of the

Device and thus that his fingerprints, face, or irises are among those that are able to unlock the device via biometric features.

40. Due to the foregoing, I respectfully request that the Court authorize law enforcement to press or swipe the fingers (including thumbs) of Hoque to the Device's fingerprint scanner, hold the Device in front Hoque's face and activate the facial recognition feature, and hold the Device in front Hoque's face and activate the iris recognition feature for the purpose of attempting to unlock the Device in order to search the contents as authorized by this warrant.

CONCLUSION

41. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ George Jasek, III
George Jasek III
Special Agent
U.S. Secret Service

Subscribed and sworn to before me
on May 17, 2019:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a white Apple iPhone with no external model number or serial numbers but marked for identification, hereinafter the "Device." The Device is currently located in the Secret Service evidence room located at 1000 Elm Street, Manchester, NH 03101.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18 U.S.C. § 1344 – Bank Fraud and Title 18 U.S.C. § 1349 – Conspiracy to Commit Bank Fraud and involve Hoque, including:

a. lists of customers and related identifying information;

b. types, amounts, prices, dates, places, and amounts of specific transactions;

c. any information related to sources of obtained victim financial information (including names, addresses, phone numbers, or any other identifying information);

d. any information recording Hoque's travel

e. all bank records, checks, credit card bills, account information, and other financial records.

f. records of Internet Protocol addresses used;

g. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

During the execution of the search of the Device described in Attachment A, law enforcement personnel are authorized to press or swipe the fingers (including thumbs) of Hoque to the fingerprint scanner of the Device, hold the Device in front of Hoque's face and activate the facial recognition feature, and hold the Device in front of Hoque's face and activate the iris recognition feature for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.